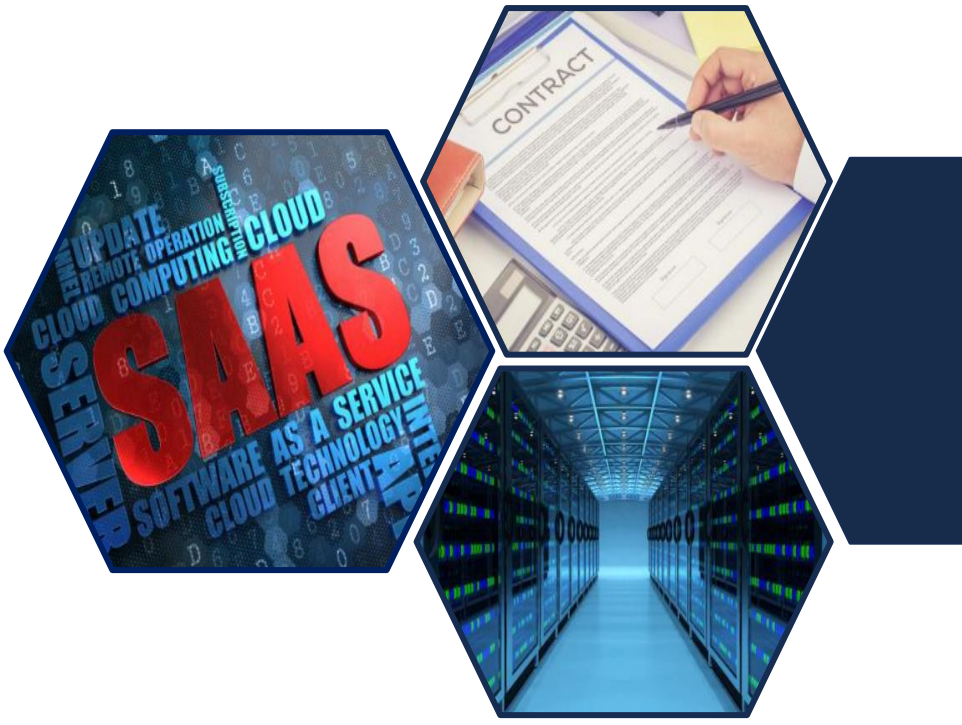
OFFICE OF INDEPENDENT INTERNAL AUDIT

DeKalb County
GEORGIA

August 2025
DeKalb County Government
County-wide

AUDIT OF CONTRACTS WITH THIRD-PARTY SOFTWARE SERVICE PROVIDERS

FINAL REPORT



Lavois Campbell, CIA, CISA, CFE, CGA
Chief Audit Executive
Office of Independent Internal Audit, Dekalb County, GA

Audit Report No. IA-2024-0200-IT

This page was intentionally left blank.

DeKalb County GEORGIA

Lavois Campbell
Chief Audit Executive

AUDIT OF CONTRACTS WITH THIRD-PARTY SOFTWARE SERVICE PROVIDERS
REPORT NO. IA-2024-0200-IT

FINAL

HIGHLIGHT SUMMARY

Why We Performed the Audit

In accordance with the OIIA's Annual Audit Plan, we audited DeKalb County's third-party SaaS and technology vendor contracts to evaluate governance, compliance, and performance. As the County increasingly relies on external providers, effective oversight—per NIST SP 800-53—is critical to mitigate risks such as data breaches, service disruptions, and financial inefficiencies. Our findings assess contract safeguards, while recommendations aim to strengthen management practices and reduce operational risks.

Audit Approach

We evaluated the Department of Innovation and Technology's (DoIT) SaaS contract processes by:

- Reviewing policies, best practices, and sample agreements.
- Conducting process walkthroughs and interviews with DoIT personnel.
- Analyzing documentation for compliance and risk management.

Background

DeKalb County's adoption of SaaS solutions supports cost efficiency, scalability, and security, aligning with DoIT's 2024-2027 Strategic Plan to transition to cloud-based infrastructure. However, third-party services introduce risks like data breaches, necessitating rigorous vendor selection, contract lifecycle management, and ongoing oversight to ensure compliance and performance.

This audit underscores the need for robust contract frameworks to safeguard County operations while leveraging third-party expertise.

What We Found

The audit noted that DoIT has developed and documented a third-party contract policy to guide vendor management; however, the policy remains in draft form and has not undergone formal review and approval. Additionally, DoIT has assigned roles and responsibilities to the Application Team for vendor management, ensuring some structure is in place for managing third-party relationships.

AUDIT OBSERVATION
1. Third-Party Contract Policy is Unapproved and Lacks Key Vendor Oversight Provisions
2. Inadequate Oversight of Third-Party SaaS Provider Controls
3. Absence of Audit Right & Independent Assessment in Agreements
4. No Provision for Incident Response, Notification & Remediation in SaaS Agreements
5. Cross-Border and Local Legal Compliance and Legal Request Handling Provisions Not Defined in SaaS Agreements.
6. Insufficient Contractual Clarity on Data Security, Custodianship, and Breach Responsibilities
7. Inadequate Definition of Data Protection and Compliance Responsibilities
8. Missing Key Provisions in SaaS Agreements Expose the County to Data and Operational Risks
9. Absence of Service Continuity Clause
10. Deficiencies in SaaS Agreements Related to Points of Contact Responsibilities and Subcontractor Lists

What We Recommend

We recommend that the DoIT management address the control process deficiencies identified in this report.

How Management Responded

Management agrees with the findings of the report and has Action plans to address them by the **2nd Quarter 2026.**

TABLE OF CONTENTS

BACKGROUND AND INTRODUCTION

The National Institute of Standards and Technology (NIST) defines *Software as a Service* (SaaS) as a cloud computing model where applications are hosted by third-party providers and accessed over the Internet. NIST emphasizes the importance of strong data protection, cybersecurity, and regulatory compliance in such environments.

Government entities like DeKalb County have increasingly adopted SaaS solutions to improve operational efficiency and service delivery. SaaS offers significant advantages, including cost-effectiveness, scalability, flexibility, and reliability—making it a key component in modernizing public sector operations.

To support this shift, the Department of Innovation and Technology's (DoIT) 2024–2027 Strategic Plan outlines a move from on-premises systems to a shared enterprise cloud infrastructure. This strategy is designed to enhance resource utilization, eliminate duplicative efforts, and foster a more responsive and agile IT environment, in alignment with the County's broader goals for operational excellence.

As the County continues to expand its reliance on SaaS platforms, the need for robust contractual protection and effective oversight grows increasingly critical. Weak or incomplete agreements—particularly those lacking in key provisions such as data security, incident response, and vendor accountability—can expose the County to legal, operational, and cybersecurity risks. Comprehensive contracts and consistent post-award monitoring are essential to ensure regulatory compliance, service continuity, and the protection of sensitive County data.

The procurement and management of SaaS services involves several key stakeholders, each with distinct responsibilities:

- **Business Unit (Contract Owner):** Identifies service needs, defines performance expectations, and manages vendor relationships on a day-to-day basis.
- **Purchasing & Contracting Department:** Oversees the solicitation, evaluation, and selection of vendors, ensuring competitive processes and compliance with County procurement policies.
- **Law Department:** Reviews and negotiates contract terms to ensure legal enforceability and alignment with the County's risk tolerance and statutory obligations.
- **Department of Innovation and Technology (DoIT):** Assesses technical compatibility, supports integration, defines service-level expectations from a technology perspective, and ensures that cybersecurity, privacy, and regulatory requirements are fully addressed within the contract.

These departments operate within a framework of County policies—such as the Procurement Policy, Third-Party Contracting Policy, and Information Security Policy—designed to guide the acquisition and management of third-party technology services.

This audit examines whether current SaaS contracts and post-award practices are adequate to manage third-party risks and uphold the County's legal, operational, and security obligations.

Why This Audit Was Performed

Government agencies across the country have faced data breaches and service disruptions due to inadequate contractual safeguards in SaaS agreements. DeKalb County is similarly at risk if vendor contracts lack key protections.

This audit was initiated to determine whether third-party service provider contracts include the necessary legal, operational, and security controls to protect the County's interests. These contracts often involve access to critical systems and sensitive information, making it vital that they align with County policies, applicable laws, and widely accepted industry standards.

Without clear provisions such as service level expectations, data protection clauses, incident response plans, and audit rights, the County may be exposed to operational disruption, reputational damage, and regulatory penalties.

By systematically reviewing these agreements, the audit helps to ensure vendors are held accountable, County data is protected, and public resources are managed responsibly.

Scope, Objectives, and Methodology

This audit focused specifically on the contract execution and post-award management phases of SaaS agreements. These stages are crucial for confirming that vendor contracts contain the necessary safeguards for performance, compliance, and data protection. Key contract elements reviewed included:

- Service Level Agreements (SLAs)
- Data protection and privacy clauses
- Incident response protocols
- Audit rights
- Termination and transition provisions

The audit also evaluated the County's ongoing ability to monitor vendor compliance and enforce contract terms throughout the contract lifecycle.

The scope of this engagement included SaaS contracts in effect between **January 1, 2023, and August 31, 2024**.

The primary objective was to assess the compliance, completeness, and effectiveness of these contracts, and to identify areas for improvement. The evaluation was based on recognized best practices from the **Information Systems Audit and Control Association (ISACA)**, **NIST Special Publication 800-53**, and the **Cloud Security Alliance**.

Audit procedures included interviews with Department of Innovation and Technology (DoIT) staff and procedural testing to evaluate current contract management processes.

AUDIT RESULTS

The Department of Innovation and Technology (DoIT) has developed a draft policy intended to guide the management of third-party vendor contracts; however, the policy remains in draft form and has not yet received formal approval. Although the six contracts reviewed as part of this audit incorporated several best-practice provisions consistent with DoIT's internal standards and the NIST framework, we identified areas where contract management processes could be further strengthened. To minimize any risk of exposure to the County, the names of the third-party applications have been intentionally omitted and replaced with the generic letters (**R, I, Y, H, S, P**). This report presents our detailed findings along with corresponding recommendations for improvement.

Finding 1: Third-Party Contract Policy is Unapproved and Lacks Key Vendor Oversight Provisions

DoIT has developed and documented policies to guide the Third-Party Service Provider Contract process. These documents include the DRAFT DeKalb County Third-Party Contract Policy. The following observations were identified from our review of the draft policy:

1. The **absence of a version history** in the Third-Party Policy made it unclear whether revisions have been made.
2. Absence of provision on the **frequency of review or update**.
3. The policies have **not been officially approved** by the County law department and County senior executives.
4. The policies **did not address periodic reviewing of third-party independent audits** or assessment reports of service providers.
5. The policy was **not fully customized for the DeKalb environment**, including references to non-existent roles within the county. For example, Section 4C of the Third-Party Contract Policy, Contract Terms and Conditions, **refers to generic roles that are non-existent at DeKalb County**. The section states, "The service provider personnel are required to report all security incidents directly to the project supervisor and {insert appropriate role}."
6. The policy **did not include a reference to related standards, policies,** and procedures.

NIST SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations provides guidelines for managing information security risks. The policy components are purpose and scope, roles and responsibilities, compliance requirements, and a timeline for periodic review and updates.

Section 2 - Purpose of the DeKalb County Third Party Contract Policy states that the purpose of this policy is to establish rules and operating parameters for third-party vendors' access to company information, their operator responsibilities, and protection of

DeKalb County assets, data, and PII. This policy supports compliance with federal and state data privacy laws.

Section 4A of the DeKalb County Third Party Contract Policy states that before entering into any agreement or contract, DeKalb County staff shall follow due diligence in selecting third-party vendors. Third parties must comply with all applicable state procurement, DeKalb County policies, practice standards, agreements, and any binding legislation at the state and federal levels.

The draft policy is awaiting comprehensive review and approval processes, leading to omissions in critical areas such as version control, formal approval, periodic assessments, and customization to DeKalb County's specific environment.

The absence of a requirement in the policy for management to review the results of third-party independent audits or assessments could result in unawareness of the County's exposure to risks such as:

- Data breaches.
- Damage to the County's reputation.
- Regulatory non-compliance.
- Loss of confidential information and cyber-attacks.

The absence of a version history made it difficult to track changes and hold anyone accountable for decisions made in policy development.

Finding 2: Inadequate Oversight of Third-Party SaaS Provider Controls

System and Organization Controls 2 (SOC 2) is a cybersecurity framework developed by the AICPA to ensure that service providers manage customer data securely, in accordance with five Trust Service Principles: security, availability, processing integrity, confidentiality, and privacy. ISACA's IS Audit/Assurance Program on Cloud Computing Control Activities C9 and C10 require service providers to make independent third-party assessment reports available to customers using recognized audit procedures and to align their operations with customer requirements.

Our review of six (6) Software-as-a-Service (SaaS) agreements and discussions with County management revealed that two of the six contracts did not have SOC 2 reports periodically obtained or reviewed by management. Vendor **S** stated that the SOC 2 report was in the observation period and would not be available until 2025. For Y Technologies, the vendor required DeKalb County to sign a non-disclosure agreement (NDA) before releasing the report. The matter has since been referred to the County's Law Department.

The Department of Innovation and Technology's (DoIT) draft third-party contract management policy does not currently require the periodic acquisition and review of independent assurance reports such as SOC 2. DoIT also cited limited staffing resources as a contributing factor to the lack of oversight.

Failure to obtain and review SOC 2 reports limits the County's visibility into the control environment of its service providers, increasing the risk of exposure to cybersecurity threats, service interruptions, data confidentiality breaches, and non-compliance with data governance standards. Additionally, the absence of proactive risk monitoring could result in operational disruptions if a provider fails to meet security or performance obligations.

We recommend that DoIT update its third-party contract management policy to require the periodic request and review of SOC 2 or similar independent assurance reports for all critical third-party providers. A centralized review schedule and responsible personnel should be established to ensure ongoing compliance.

Finding 3: Absence of Audit Right & Independent Assessment in Agreements

DeKalb County Code of Ordinances, Section 10A, requires all contracts with outside contractors and subcontractors to include a "right-to-audit" clause. ISACA's IS Audit/Assurance Program on Cloud Computing Control Activities C15 and C16 require that service provider contracts permit the customer to conduct independent assessments and that providers submit third-party reviews performed by recognized audit organizations. DeKalb County's internal procurement guidance also states that service providers are expected to comply with all County audit requirements.

During our review of six SaaS agreements, we found that the agreement with vendor **I** lacked audit rights clauses. In addition, five of the six agreements did not include provisions requiring independent assessments such as SOC 2. Only the agreement with vendor **P** included a clause addressing SOC compliance.

This issue appears to be the result of the absence of a standardized pre-contract checklist and insufficient legal and procurement coordination during contract development.

Without these clauses, the County lacks contractual authority to monitor, assess, or demand transparency from its vendors. This exposes the County to significant risks, including undetected control weaknesses, regulatory non-compliance, data breaches, and reputational harm.

Finding 4: No Provision for Security Incident Response, Notification & Remediation in SaaS Agreements

During discussions with key personnel from the Department of Innovation and Technology (DoIT) and our review of a sample of six SaaS agreements, **we identified gaps in how security incidents, incident investigation, and notification responsibilities are addressed within the contracts.** The following table highlights the key findings noted:

Vendor Agreements - Incident Response, Notification & Remediation Clauses

Vendor	Incidents & Events	Responsibilities for the investigation of incidents	Notification Procedures according to Local Laws
R	❌ No	❌ No	❌ No
I	✅ Yes	❌ No	❌ No
Y	✅ Yes	❌ No	❌ No
H	✅ Yes	✅ Yes	✅ Yes
S	❌ No	❌ No	❌ No
P	✅ Yes	✅ Yes	✅ Yes

Source of Control area: ISACA & DeKalb Third Party Policy
Legend: ✅ Compliant | ❌ Not Addressed

- ***Section 4 C. Third-party contract terms and provisions* of the third-party contract policy, Pg 2, No 11: Requires** that service provider personnel report all security incidents directly to the project supervisor. Security incident management responsibilities and details must be specified in the contract agreement and specific to data incident/breach notification, procedures, notifications, and remedies.
- **NIST SP 800-161r1-upd1 IR**-5 (Incident Monitoring): Enterprises should ensure that agreements with suppliers include requirements to track and document incidents, response decisions, and activities
- **ISACA Control Activities C1 of the IS Audit/Assurance program on cloud computing requires: The contract describes specific definitions of incidents (data breaches, security violations) and events (suspicious activities),** and the actions to be initiated by and the responsibilities of both parties.

DoIT Management explained that the absence of the clauses is because the terms and conditions for some large vendors are non-negotiable.

The lack of incident response, notification, and remediation responsibilities may result in incomplete resolution of security breaches, leaving organizations exposed to recurring issues and increased vulnerabilities.

Finding 5: Cross-Border and Local Legal Compliance and Legal Request Handling Provisions Not Defined.

ISACA Control Activities C14 of the IS Audit/Assurance program on cloud computing requires that legal compliance with local and cross-border laws is defined as a component of software as a service vendor contracts. Through interviews and a review of SaaS agreements, we noted the following:

Provisions not Defined in Contracts	R	I	Y	H	S	P
Cross-Border and Local Legal Compliance	❌	✅	✅	✅	✅	✅
Handling subpoenas, service of process, and other legal Requests	❌	✅	✅	❌	✅	✅

Source of Control area: ISACA & DeKalb Third Party Policy
Legend: ✅ Compliant | ❌ Not Addressed

DoIT management stated that the missing contract clauses were because agreements with some vendors are not negotiable.

The absence of defined legal compliance measures may expose the organization to non-compliance risks, particularly in international and multi-jurisdictional contexts. Failure to address cross-border and local law compliance can lead to non-compliance with regulations, resulting in legal penalties, regulatory sanctions, operational disruptions, increased legal risks, and financial liabilities. Additionally, the absence of a unified process for handling subpoenas and legal requests heightens the risk of unauthorized disclosure of sensitive information, potentially violating data privacy regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

The GDPR governs data protection and privacy for individuals within the European Union (EU) and the European Economic Area (EEA). At the same time, the CCPA enhances privacy rights and consumer protection for California residents. Violations of these regulations could result in substantial fines, litigation, and significant reputational damage.

Finding 6 – Insufficient Contractual Clarity on Data Security, Custodianship, and Breach Responsibilities

During discussions with key personnel from the Department of Innovation and Technology (DoIT) and a review of a sample of Software-as-a-Service (SaaS) agreements, it was observed that several agreements lacked comprehensive provisions related to data protection and security responsibilities. Specifically, key clauses addressing discovery

searches, litigation holds, transfer of custodianship, performance monitoring, and encryption requirements were either absent or inadequately defined.

The following table summarizes the compliance status of each vendor contract with respect to ten recommended data security and custodianship provisions:

Contract Clause	R	I	Y	H	S	P
1. Contractual Agreement Responsibilities	❌	✅	✅	❌	❌	❌
2. Guardianship of Customer Data	✅	✅	✅	✅	❌	✅
3. Transfer of Data Custodianship	✅	✅	✅	❌	❌	✅
4. Term Negotiation and Transition from Processing	✅	✅	✅	✅	✅	✅
5. Data Breach Responsibilities	✅	✅	✅	❌	❌	✅
6. Customer Access to Performance and Vulnerability Testing	❌	✅	✅	❌	❌	✅
7. Encryption Requirements	❌	✅	❌	❌	✅	✅
8. Issue Monitoring Processes	✅	❌	❌	❌	✅	✅
9. DoIT Internal Issue Monitoring	❌	✅	❌	❌	✅	✅
10. Data Protection Policies	❌	✅	❌	❌	❌	✅

Source of Control area: ISACA & DeKalb Third Party Policy

Legend: ✅ Compliant | ❌ Not Addressed

According to ISACA Control Activities C12 and C13 from the IS Audit/Assurance Program on Cloud Computing, contracts should be reviewed by key stakeholders to ensure all critical legal, financial, and security obligations are clearly defined, and the customer must monitor compliance with these obligations.

In addition, NIST SP 800-161r1 recommends that contracts include clear provisions for data transmission integrity (SC-8), protection of data at rest (SC-28), and access to vulnerability and issue monitoring data to manage cybersecurity risk in third-party relationships.

The absence of defined data protection processes, encryption requirements, transition responsibilities, and access to performance and vulnerability tests increases the risk of data breaches, regulatory non-compliance, litigation, operational disruptions, data integrity issues, and the inability to verify the security and reliability of the service provider.

Finding 7: Inadequate Definition of Data Protection and Compliance Responsibilities

During our audit of SaaS agreements executed between January 1, 2023, and August 31, 2024, we evaluated whether the use of cloud computing meets established customer compliance requirements. Discussions with key personnel from DoIT revealed significant gaps in the contractual scope for data protection responsibilities. Our review identified the following issues:

1. **Undefined Data Protection Responsibilities:**
   In three vendor agreements (**R, Y,** and **H**), there is no specification that data protection responsibilities should be based on the risk associated with the deployment scenario.
2. **Absence of a Clause Assigning Responsibilities:**
   Vendor **H** agreement lacks a clause that clearly assigns data protection responsibilities between the County and the service provider.
3. **Lack of Explicit Data Protection Measures:**
   The agreement with vendor **S** does not detail the specific data protection measures that each party (the County and the service provider) is expected to implement.

According to ISACA Control Activity C19 from the IS Audit/Assurance program on cloud computing, contracts must clearly delineate data protection responsibilities based on the deployment scenario (SaaS, PaaS, IaaS). **The failure to define these responsibilities increases the risk of mishandling sensitive data, potentially leading to regulatory non-compliance, data breaches, and related legal, financial, and reputational consequences.**

Finding 8: Missing Key Provisions in SaaS Agreements Expose the County to Data and Operational Risks

A sample of six (6) SaaS agreements executed between January 1, 2023, and August 31, 2024, was reviewed during the audit. The audit also included an examination of the Third-Party Contract Policy, and the Information Security Policy (ISP) dated May 2, 2024. Discussions were held with key Department of Information Technology (DoIT) personnel.

The draft Third-Party Policy specifies 12 contractual requirements or control areas. In addition, we considered the protection of county data from unauthorized AI model training. The audit revealed widespread inconsistencies across SaaS agreements, with critical gaps in data protection, access control, and confidentiality provisions—posing significant operational and security risks to the County. The audit team observed the following non-compliance with the following 10 of the thirteen control areas specified in the county policy:

SaaS Agreement Compliance Summary by Control Areas

#	Control Area	Compliant Agreements	Non-Compliant Agreements	Non-Compliance Ratio	Notes (Condition + Risk/Impact)
1	**Data Destruction / Disposal**	✅ 3/6	R, Y, H	❌ 3/6	**Condition:** 3 agreements lacked clauses for secure data disposal at contract end. **Risk:** Increases the likelihood of data retention, leakage, or unauthorized reuse.
2	**Non-Disclosure Agreement (NDA)**	✅ 5/6	Y	❌ 1/6	**Condition:** NDA clause was missing from Tyler's agreement. **Risk:** Weakens protection of confidential information and legal recourse options.
3	**Security Clearance for PII Access**	✅ 2/6	R, I, H, S	❌ 4/6	**Condition:** 5 agreements had no requirement for staff clearance when accessing PII. **Risk:** Heightens exposure to unauthorized access and privacy breaches.
4	**Restriction of Info Usage (including AI Training Risk)**	⚠️ 6/6	R, I, Y, H, P, S	❌ 0/6	**Condition:** All the agreements had provisions restricting information usage without approval. No agreements specifically restricted the use of confidential data in AI model training. **Risk:** Sensitive data may be used to train AI systems without consent.
5	**User Provisioning**	✅ 4/6	H, P	❌ 2/6	**Condition:** User Provisioning processes were not included in 2 agreements. **Risk:** May lead to uncontrolled or unauthorized access to systems or data.
6	**System Monitoring**	⚠️ 2/6	R, I, Y, H	❌ 4/6	**Condition:** 5 agreements lacked system monitoring clauses. **Risk:** Reduces visibility into vendor activities and limits breach detection capabilities.
7	**Remote Access Procedures**	⚠️ 2/6	R, I, H, S	❌ 4/6	**Condition:** 5 vendors did not specify secure remote access tools or protocols. **Risk:** Increases exposure to external cyber threats and unauthorized access.
8	**Change Management**	✅ 5/6	I	❌ 1/6	**Condition:** NICE agreement lacked change control provisions. **Risk:** Increases risk of unauthorized or undocumented changes to systems or services.
9	**Access Role Specification**	❌ 0/6	All	❌ 6/6	**Condition:** None of the agreements defined roles or job functions with system access. **Risk:** Leads to over-provisioning and lack of accountability.
10	**Activation of confidential data when required**	✅ 2/6	R, I, Y, H	❌ 4/6	**Condition:** 5 vendors did not specify PII data activation when required. **Risk:** This could result in unauthorized access and legal consequences

Legend: ✅ Compliant | ⚠️ Weak or Partially Present | ❌ Not Addressed

Control Area Compliance Summary by Vendor Contract

Vendor	Data Disposal	NDA	PII Clearance	Confidential Use	User Provisioning	System Monitoring	Remote Access	Change Mgmt.	Data Activation	Role Access
R	❌	✅	❌	❌	✅	❌	❌	✅	❌	❌
I	✅	✅	❌	❌	✅	❌	❌	❌	❌	❌
Y	❌	❌	✅	❌	✅	❌	⚠️	✅	❌	❌
H	❌	✅	❌	❌	❌	❌	❌	✅	❌	❌
S	✅	✅	❌	❌	✅	⚠️	❌	✅	✅	❌
P	✅	✅	✅	❌	✅	⚠️	⚠️	✅	✅	❌

Source of Control area: ISACA & Dekalb Third Party Policy

Legend: ✅ Compliant | ⚠️ Weak or Partially Present | ❌ Not Addressed

Section 2.8.1 Third Party Access par. 7 of the **Information Security Policy** states that Third parties with access to DeKalb County's Confidential and Sensitive information shall have the appropriate clearance to handle that information. Third parties will ensure that all Confidential or Sensitive information is collected and returned to DeKalb County or destroyed within 24 hours in the event of separation or termination of third-party employment.

The absence of these key requirements could be attributed to the lack of a pre-contract checklist or contract template to assist management in verifying the completeness and accuracy of agreements/contracts.

The consequences of not including some key terms and provisions in the contract are the disclosure of sensitive information, loss of rights, lack of control over service provider activities, and the increased likelihood of unapproved changes and operational disruptions.

Finding 9: Absence of Service Continuity Clause

During our review of six (6) SaaS agreements and Service Level Agreements (SLAs), we identified that **four (4) agreements (R, Y, S, and P) did <u>not</u> include provisions addressing service continuity in the event of vendor acquisition or changes in management.** Key best practice recommendations include:

- **Control ID BCR-01 of the Cloud Control Matrix V3.0.1, developed by the Cloud Security Alliance (CSA),** recommends business continuity management and operational resilience. Requirements for business continuity plans include the following:
  - Defined lines of communication, roles, and responsibilities
  - Detailed recovery procedures, manual workaround, and reference information
  - Method for plan invocation

- **Control ID BCR-03 of Cloud Control Matrix** version 4, developed by the Cloud Security Alliance, recommends businesses to establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.
- **ISACA Control Activities C3 of the IS Audit/Assurance program** on cloud computing recommends SLAs that support the business requirements are defined, accepted by the service provider, and monitored by both parties.

The County relies on the standard SLA terms provided by the vendors. These SLAs undergo internal review and are then submitted to the County law department for approval, with limited opportunity for negotiation. These vendors typically offer pre-defined SLA terms, which limit the County's ability to customize agreements to address critical concerns like service continuity in the event of vendor acquisition or management changes.

The lack of service continuity provisions in SLAs poses a risk of operational disruptions, data loss, or reduced service quality in the event of vendor acquisition or management changes. This lack of foresight in governance could lead to downtime or service delivery interruptions, impacting critical organizational functions.

Finding 10: Deficiencies in SaaS Agreements Related to Points of Contact Responsibilities and Subcontractor Lists

A review of **six (6) active Software as a Service (SaaS) agreements** from January 1, 2023, to August 31, 2024, identified deficiencies related to point-of-contact designation and subcontractor list maintenance. These gaps pose risks in compliance, accountability, and security. The audit scope also included a detailed examination of the DeKalb County Third-Party Contract Policy, the Information Security Policy (ISP) dated May 2, 2024, and discussions with key personnel from the Department of Information Technology (DoIT). According to **Section 4B of the DeKalb County Third-Party Contract Policy**, the County must maintain copies of all agreements with service providers, as appropriate. In addition, vendors **must:**

- Designate a responsible point of contact for contract terms and service implementation.
- Provide a detailed list of subcontracted providers and their services.
- Comply with applicable state and federal laws and internal policies.

The table below summarizes the compliance status for the reviewed SaaS agreements regarding the designation of points of contact and the maintenance of subcontractor lists:

Vendor	Point of Contact Responsibilities?	Subcontractors Listed?
R	✅ Yes	❌ No
H	✅ Yes	❌ No
I	❌ **No**	❌ No
Y	❌ **No**	❌ No
P	✅ Yes	❌ No
S	✅ Yes	✅ Yes
Vendor Compliant	**4/6 (67%)**	**1/6 (17%)**

Absence of a clearly identified Point of Contact Responsibilities may result in communication delays, ineffective issue resolution, and decreased accountability. Lack of transparency regarding subcontractors handling sensitive County data significantly increases compliance, accountability, and security risks.

Potential causes identified include the following:

- The absence of a standardized pre-contract checklist has resulted in inconsistent compliance with agreement terms.
- Section 4B requirements are inadequately enforced, permitting contracts lacking key compliance elements to proceed.
- Vendors may not fully understand their contractual obligations, particularly the importance of subcontractor disclosure.

RECOMMENDATIONS AND MANAGEMENT RESPONSE FOR ALL 10 FINDINGS

We recommend that DoIT management work with **relevant stakeholders (Law, Purchasing & Contracting Department, Office of the Chief Operating Officer (COO))** to address each of the following recommendations.

Rec	Recommendation	Related Findings
R1	Finalize and approve the Third-Party Contract Policy. Include version control, scheduled reviews (e.g., biennially), clear stakeholder roles, and reference to internal and external standards. Submit to the County Attorney and the COO for approval. The policy should be updated to specifically require and support the following recommendations: R3-R13.	**Finding 1**
Management Agreement	***Description of Management's Action Plan to Address Finding***	***Estimated Timeline to implement Action Plan***
✅ **Agree** ☐ **Disagree**	DoIT will provide a draft of the policy for approval. Approval from law will take 60-90 days. DoIT will have a draft in 45 days.	4th Quarter 2025

Rec	Recommendation	Related Findings
R2	Develop and enforce a standardized SaaS contract template. Include clauses addressing R4 to R12. In addition, ensure recommended provisions in **Appendix 4** are included. **Use as baseline for all future contracts and renewals of existing contracts.**	**Findings 1–10**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT will work with Law & Purchasing to draft a standard SaaS contract template.	1st Quarter 2026

R3	Implement a mandatory pre-contract checklist embedded in procurement processes. Validate point of contact, subcontractor disclosures, risk ownership, audit rights, and legal obligations. Develop a vendor onboarding module to educate vendors on County requirements and obligations.	**Findings 1, 2, 3**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT will implement the recommended checklist.	1st Quarter 2026

R4	Require vendors (via contact) to submit annual SOC 2 or equivalent third-party assurance reports. Assign a team to track receipt, review reports, and initiate follow-up for exceptions. Establish a central review calendar.	**Findings 2, 6, 7**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT agrees , and the GRC officer in R-12 will assume the actions above. DoIT will request GRC resource in FY26 budget.	2nd Quarter 2026
***Additional Comments**:* Contingent upon the resource being approved in the 2026 budget.		

Rec	Recommendation	Related Findings
R5	DoIT Management should collaborate with the Law and Purchasing & Contracting Department to include "right-to-audit" clauses and independent assessment terms in all contracts. For legacy contracts, require amendment at renewal or establish legal exceptions and controls.	**Findings 2, 7**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT will work with the law to address as a part of the standardized SaaS contract template.	1st QTR 2026

R6	DoIT Management should collaborate with the Law and Purchasing & Contracting Department to mandate that all contracts include clauses defining incident types, investigation responsibilities, breach timelines, and reporting paths per law.	**Finding 4**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT will work with the law to address as a part of the standardized SaaS contract template.	1st QTR 2026

R7	DoIT Management should collaborate with the Law and Purchasing & Contracting Department to clearly define data custodianship, encryption (at rest and in transit), breach accountability, litigation hold requirements, and post-termination data handling in all contracts.	**Findings 3, 9, 10**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT will work with law to address clause additions,	1st QTR 2026

Rec	Recommendation	Related Findings
R8	DoIT Management should collaborate with the Law and Purchasing & Contracting Department, including provisions addressing cross-border data flow, local legal compliance (e.g., GDPR, CCPA), and legal request handling (e.g., subpoenas, service of process).	**Finding 8**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT will work with law and Purchasing to address as a part of standardized SaaS contract template.	1st QTR 2026

R9	Use a shared responsibility matrix (SRM) in each SaaS agreement. Define whether County or vendor owns each responsibility area (e.g., access controls, backups, data classification). Tailor to service model (SaaS, PaaS, IaaS).	**Findings 3, 9, 10**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT will work with law to address as a part of standardized SaaS contract template.	1st QTR 2026

R10	Require all vendors to provide continuity and transition plans in the event of acquisition or leadership change. **Include**: Notification within **60–90 days in advance**, or within **30 days post-close** where advance disclosure is restricted. Use a supplemental addendum to capture DeKalb-specific continuity requirements when vendor SLAs are non-negotiable.	**Findings 5**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT will work with law to address as a part of standardized SaaS contract template.	1st QTR 2026

Rec	Recommendation	Related Findings
R11	Ensure contracts define user provisioning, role-based access control, secure remote access, system monitoring, and change management procedures. Include these in technical annexes or SLAs.	**Findings 3, 10**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT will work with law to address as a part of standardized SaaS contract template.	1st QTR 2026

R12	Assign clear contract oversight responsibility within DoIT. If needed, create a Governance, Risk, and Compliance (GRC) Officer role to manage third-party policy enforcement, risk reporting, and contract compliance.	**Finding 5**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT agrees, and the GRC officer in R-12 will assume the actions above. DoIT will request GRC resources in FY26 budget.	2nd QTR 2026
***Additional Comments**:* Contingent upon resources approved in 2026 budget.		

R13	Create and maintain a **Cloud Risk Register** for contracts that can't be amended due to vendor constraints. Capture unmitigated risks, compensating controls, and document executive approvals or exceptions. Submit the risk register to the Chief Executive Officer or designee for approval.	**Findings 1–10**
Management Agreement	***Description of Management's Action Plan to Address the Finding***	***Estimated Timeline to implement Action Plan***
☑ **Agree** ☐ **Disagree**	DoIT agrees and will create the risk register.	1st QTR 2026

APPENDICES

Appendix I – Purpose, Scope, and Methodology

Purpose

The purpose of this audit was to assess the governance, operational efficiency, compliance, accuracy, and overall effectiveness of the County's third-party service provider contracts, ensuring their alignment with DeKalb County's third-party contract policy and best practices.

Scope and Methodology:

The scope of this engagement focused on the County's third-party contract with software-as-a-service (SaaS) providers from January 1, 2023, to August 31, 2024

Our methodology included but was not limited to the following:

- Researched related best practices.
- Reviewed the County's Third-party contract policies and procedures.
- Selected and tested a sample of SaaS agreement
- Conducted a walkthrough of the Third-Party Service Provider Contract processes.
- Reviewed applicable documentation and information.
- Interviewed appropriate County personnel in the Department of Innovation and Technology (DoIT)

Appendix II – Management Response

DeKalb County GEORGIA

Department of Innovation & Technology
www.dekalbcountyga.gov

August 19, 2025

Lavois Campbell
Chief Audit Executive
Office of Independent Internal Audit
1300 Commerce Drive, Suite 300
Decatur, Georgia 30030

RE: Management Response Audit of Contracts with Third-Party Software Services Providers - IA-2024-0200-IT

Dear Mr. Campbell:

In accordance with DeKalb County, Georgia – Code of Ordinances / Organizational Act Section10A- Independent Internal Audit, this is our response to the audit named above provided in this document. As required by the ordinance, our response includes 1) a statement regarding our agreement or disagreement along with reasons for any disagreement, 2) our plans for implementing solutions to issues identified, and 3) the timetable to complete such plans.

If you have any questions about this response, please contact Felecia Green, Deputy Chief Information Officer, DoIT.

Sincerely,

Felecia A. Green

Felecia Green, Deputy Chief Information Officer, DoIT

Appendix III – Definitions and Abbreviations

Acronyms and Abbreviation

DoIT: Department of Innovation and Technology**.**

OIIA: Office of Independent Internal Audit.

SaaS: Software as a Service

ISP: Information Security Policy

ISACA: Information Systems Audit and Control Association

NIST: National Institute of Standards and Technology

CCM: Cloud Control Matrix

SLA: Service Level Agreement

CSA: Cloud Security Alliance

Key Definitions

Software as a Service (SaaS): SaaS is a cloud computing model in which applications are hosted by a third-party provider and made accessible to users online. SaaS solutions offer cost-effectiveness, scalability, flexibility, and enhanced security. However, they also require stringent security measures and regulatory compliance to protect sensitive data.

Service Level Agreement (SLA): An SLA is a formal contract between a service provider and a customer that defines both parties' expected service standards, performance metrics, and responsibilities. It typically includes provisions related to uptime guarantees, data security, incident response, and penalties for service disruptions.

Appendix IV – SaaS Contract Template Checklist.

Please note: The information below is intended to provide guidance on high-risk control areas that should be considered for inclusion in the contract. These are not actual contract clauses, nor are they exhaustive of all required provisions. Final contract language will be developed and approved by management in consultation with appropriate stakeholders, at management's discretion.

Control Area	Clause Guidance Description
1. Governance of Cloud Computing Services (Source: COBIT 5 EDM01; EDM05; APO13; MEA01)	a. SLAs should explicitly reflect the organization's business objectives, risk tolerance, and service criticality to ensure services meet operational needs.
	b. Include specific, measurable service level metrics (e.g., uptime %, incident response time). These metrics must allow effective monitoring and early issue detection.
	c. The SLA should contain provisions ensuring continued service in case of vendor acquisition, restructuring, or leadership change. Include data handover and exit plans.
	d. Clearly define and document governance roles and responsibilities for both the service provider and customer, including decision rights and review processes.
	e. The SLA should clearly define the reporting relationships between the service provider and the customer, outlining the roles, responsibilities, and accountability structures within each organization's governance framework.
2. Third-party Management (Source: COBIT 5 APO10; MEA02)	f. The service provider should regularly undergo independent third-party assessments, with reports made available to the customer upon request to demonstrate ongoing compliance with security, operational, and performance standards.
	g. Third-party assessment reports should include detailed evaluations of the service provider's processes for incident management, business continuity and disaster recovery, data backup, and use of co-location facilities.
	h. The service provider should conduct regular internal reviews to assess adherence to its own policies and procedures and maintain metrics that demonstrate the effectiveness and availability of key control processes.
3. Legal and Electronic Discovery (Source: COBIT 5 APO09; APO10; MEA02; MEA03)	i. The contractual agreement must define both parties' responsibilities regarding discovery searches, litigation holds, evidence preservation, and expert testimony.
	j. Service provider contract requires assurance to the customer that their data are preserved as recorded, including the primary data and secondary information (metadata and logs).
	k. Service providers understand their contractual obligations to provide guardianship of the customer's data.
	l. The customer's duty of care must cover the full contract lifecycle, including: - Precontract due diligence - Contract term negotiation - Transfer of data custodianship - Contract termination or renegotiation - Transition from processing
	m. The agreement should clearly outline each party's obligations in the event of both expected and unexpected termination—during, at the conclusion of, and after the contract period.
	n. Contractual terms must explicitly assign responsibilities for managing suspected data breaches, including reporting, investigation, and remediation duties for both parties.
	o. The customer must retain the right to regularly access the service provider's performance metrics and results of vulnerability testing.

Control Area	Clause Guidance Description
	p. The agreement must define the rights and obligations of both parties during transition periods, including the conclusion of services and post-contract data handling.
	q. The contract must define encryption standards for data in transit, at rest, and in backup systems, consistent with industry best practices.
	r. Agreements must clarify data retention periods and affirm the customer's ownership of intellectual property and associated data assets.
	s. Contractual clauses must include data protection controls to safeguard personal data in compliance with relevant privacy regulations. t. Prohibit the use of county data for training AI models without the express written consent of the county.
	u. An issue monitoring mechanism must be established to regularly review and assess the service provider's performance and risk posture.
	v. Clause requiring the customer to implement internal monitoring processes to ensure its own compliance with contractual obligations and identify potential deficiencies.
4. Legal Compliance (Source: COBIT 5 APO09; APO10; MEA02)	w. Ensure compliance with all cross-border and local laws
	x. Provision that Service provider and customer have an agreed-upon unified process for responding to subpoenas, service of process and other legal requests.
5. Right to Audit (Source: County Organizational Act, Sec. 10A (h), COBIT 5 APO09; MEA03)	y. Incorporate Right to audit clause z. Provision that audit activities should not be restricted or curtailed.
6. Compliance Scope (Source: COBIT 5 APO10; APO13; DSS01; DSS05; DSS06)	aa. Responsibilities for complying with data protection laws should be considered.
	bb. Assignment of responsibilities. Clearly defined responsibilities between the parties.
	cc. Customer and service provider each have established appropriate data protection measures within the scope of their responsibilities. The agreement should clearly establish appropriate data protection measures within the scope of the responsibilities of the customer and service provider.
7. Valid Contract (COBIT 5: EDM01; EDM05)	dd. Contract templates to ensure they include fields for signatures by both parties, and a defined contract period.
	ee. Presence of signatures by both parties. Clear indication of the contract period.
8.General Vendor Responsibilities (Source: Dekalb Third Party Contract Policy)	ff. Include defined responsibilities for the point of contact
	gg. List of all subcontracted providers should be incorporated
	hh. Defined responsibilities for the investigation of incidents
	ii. Provision of copies of agreements with subcontractors
9.Terms and Conditions (Dekalb Third Party Contract Policy)	jj. Include confidentiality terms to protect DeKalb County confidential information and PII.
	kk. Requirement that data destruction/disposal upon contract termination
	ll. Provision that data destruction/disposal is incorporated independent assessment report
	mm. Requirement on restriction of information usage
	nn. Non-disclosure agreement should be incorporated
	oo. Security clearance requirement for staff who require access to PII

Control Area	Clause Guidance Description
	pp. Requirement that third party access to confidential data shall be activated when needed
	qq. User provisioning with role-based access control
	rr. Service provider access to system and software shall be monitored for security threats and vulnerabilities by DoIT
	ss. Service providers with remote access use prescribed tools and procedures to access system remotely
	tt. Changes to applications shall be in line with DeKalb County process
	uu. List of employees with their roles and responsibilities granted access to the application. Provision that list of employees with their roles and responsibilities granted access to DeKalb County information systems shall be provided upon request.
10. Incident Response, Notification and Remediation (Dekalb Third Party Contract Policy and COBIT V MEA02)	vv. Incidents and events are clearly defined and responsibilities assigned
	ww. Responsibilities for the investigation of incidents are defined
	xx. Notification procedures according to local laws are incorporated into the incident and event process

DISTRIBUTION

Action Distribution:

Scott Shelton, CIO, Department of Innovation & Technology
Felecia Green, Deputy CIO, Department of Innovation & Technology

Statutory Distribution:

Lorraine Cochran-Johnson, Chief Executive Officer

Robert Patrick, Board of Commissioners District 1

Michelle Long Spears, Board of Commissioners District 2

Nicole Massiah, Board of Commissioners District 3

Chakira Johnson, Board of Commissioners District 4

Mereda Davis Johnson, Board of Commissioners District 5

Ted Terry, Board of Commissioners Super District 6

LaDena Bolton, Board of Commissioners Super District 7

Tanja Christine Boyd-Witherspoon, Chairperson, Audit Oversight Committee

Adrienne T. McMillion, Vice-Chairperson, Audit Oversight Committee

Lisa Earls, Audit Oversight Committee

Michael Lopata, Audit Oversight Committee

Petrina Bloodworth, Audit Oversight Committee

Information Distribution:

Dr. G. Leah Davis, CEO's Chief of Staff

Zachary L. Williams, Chief Operating Officer/ Executive Assistant

William “Bill” Linkous III, County Attorney

Dionne McKenzie – Clerk, Board of Commissioners

PROJECT TEAM

This report was submitted by:

08/20/2025

Tolu Ologbenla, MBA, CISA, CISM, CCAK, PMP, CSM
IT Internal Auditor, Senior
Office of Independent Internal Audit

Date

This report was reviewed by:

maxwell Addico

08/20/2025

Maxwell Addico, MBA, CISA, ISO/IEC 27001 LA
IT Audit Manager
Office of Independent Internal Audit

Date

The report was approved by:

Lavois Campbell

8.20.2025

Lavois Campbell, CIA, CISA, CFE, CGA
Chief Audit Executive
Office of Independent Internal Audit

Date

STATEMENT OF ACCORDANCE

Statement of Accordance

The mission of DeKalb County is to make the priorities of the citizens of DeKalb County; the priorities of County government - by achieving a safer DeKalb, building stronger neighborhoods, creating a fiscally accountable and more efficient county government, and uniting the citizens of DeKalb County.

The mission of the Office of Independent Internal Audit is to provide independent, objective, insightful, nonpartisan assessment of the stewardship or performance of policies, programs, and operations in promoting efficiency, effectiveness, and integrity in DeKalb County.

This performance audit was prepared pursuant to DeKalb County, Georgia – Code Ordinances/Organizational Act Section10A- Independent Internal Audit. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report is intended for the use of the agency to which it was disseminated and may contain information that is exempt from disclosure under applicable law. Do not release without prior coordination with the Office of Independent Internal Audit.

Please address inquiries regarding this report to the Office of Independent Internal Audit at 404-831-7946.